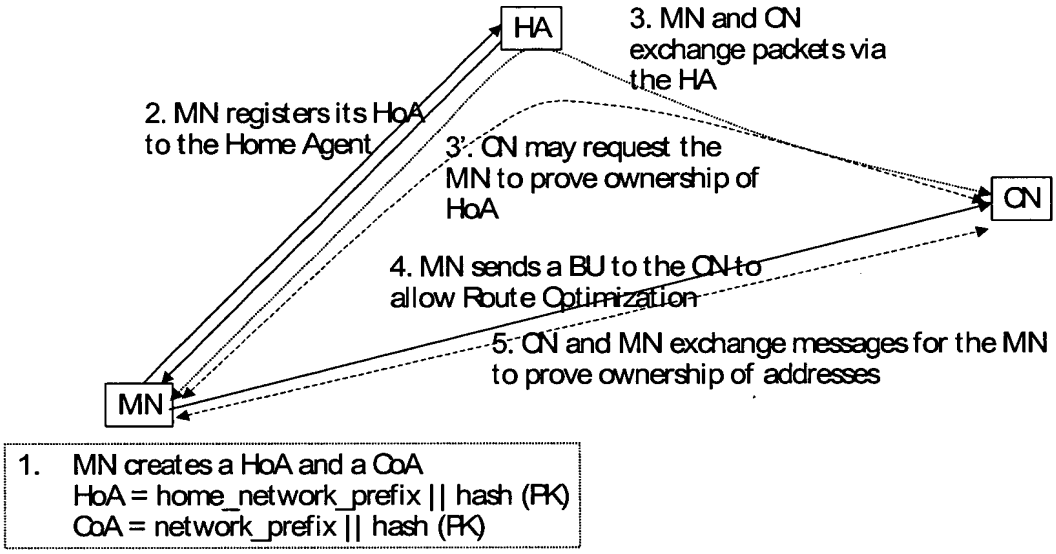

Target: the MN proves its address ownership in t executions of a 3-pass protocol

FIG. 1

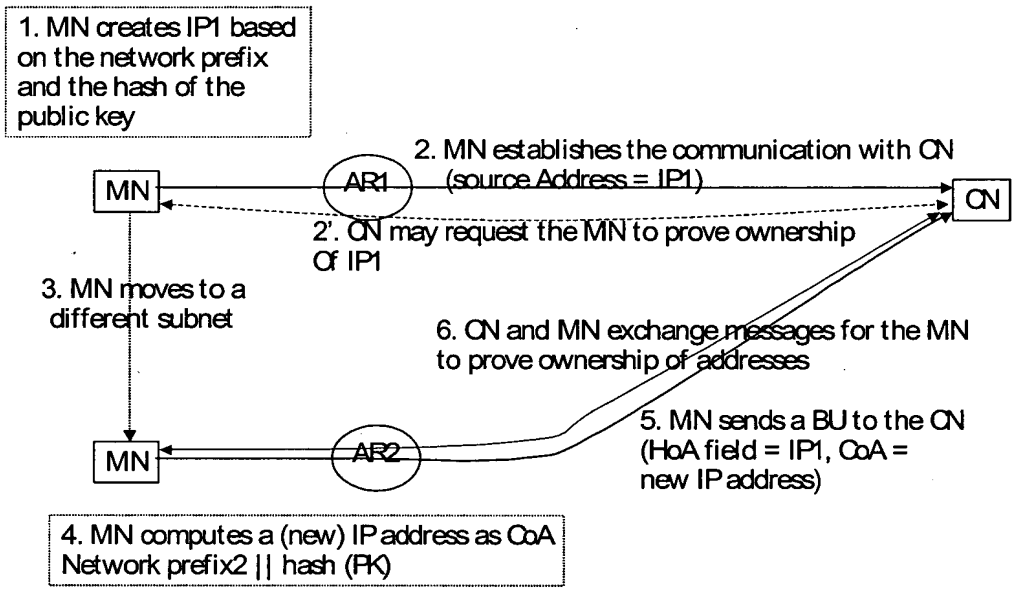
1. MN creates IP1 based on the network prefix and the hash of the public key
2. MN establishes the communication with CN (source Address = IP1)
MN
AR1
CN
2'. CN may request the MN to prove ownership Of IP1
3. MN moves to a different subnet
6. CN and MN exchange messages for the MN to prove ownership of addresses
5. MN sends a BU to the CN (HoA field = IP1, CoA = new IP address)
MN
AR2
4. MN computes a (new) IP address as CoA Network prefix2 || hash (PK)

FIG. 2

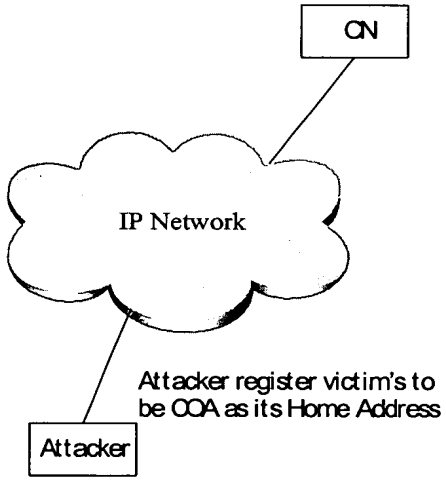
CN
IP Network
Attacker register victim's to be COA as its Home Address
Attacker

FIG. 3

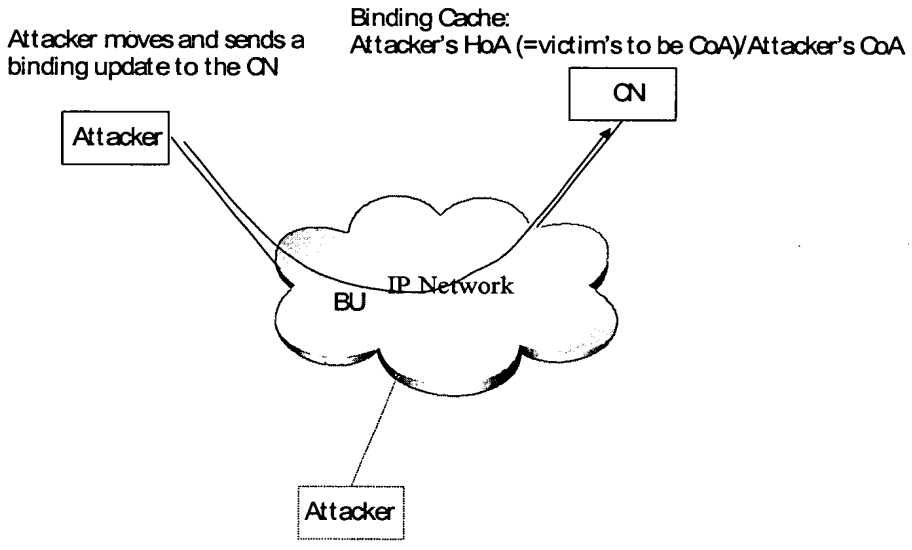
Attacker moves and sends a binding update to the CN
Binding Cache:
Attacker's HoA (=victim's to be CoA)/Attacker's CoA
CN
Attacker
IP Network
BU
Attacker

FIG. 4

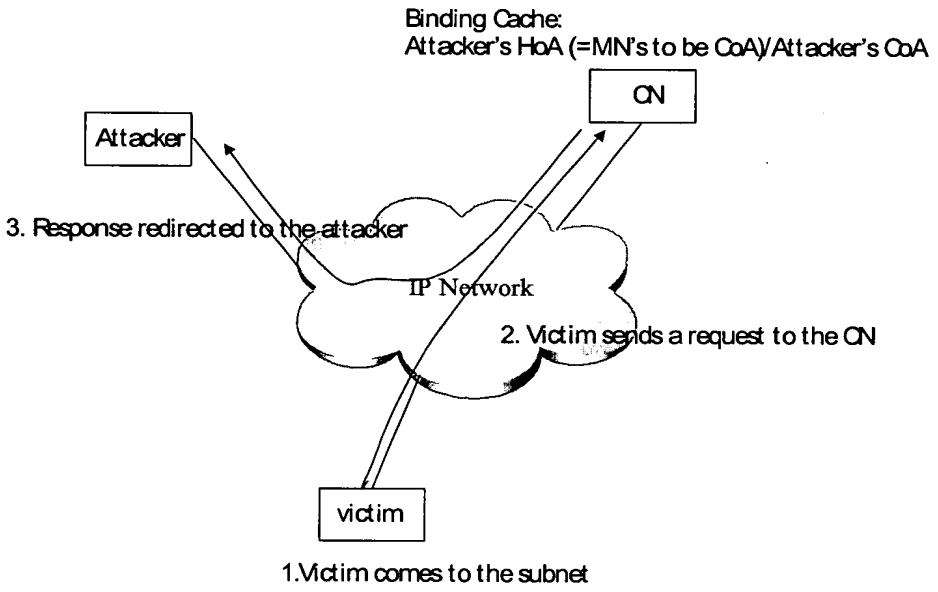
Binding Cache:
Attacker's HoA (=MN's to be CoA)/Attacker's CoA
CN
Attacker
3. Response redirected to the attacker
IP Network
2. Victim sends a request to the CN
victim
1.Victim comes to the subnet

FIG. 5